Previous Section

5.0 -- CITIS Development

The primary requirement for creating a successful CITIS is preliminary planning. The contractor and the Government must discuss and agree upon a large number of issues before the CITIS development is begun. An Integrated Product Team (IPT) for CITIS development should be formed at this time. The IPT serves as an excellent forum to address developmental issues between the Government and participating contractors. Both sides must understand exactly which functions are required and how the Government intends to utilize them. They must discuss the hardware, software, and networks that will be used, how the CITIS should handle data in different formats, and how the contractor should handle major changes in the Government's computer infrastructure.

5.1 -- CITIS Development Strategy

During the planning phase of the CITIS development process, contractors must determine their strategy in terms of the location/distribution of the program-specific data repository, the extent to which their suppliers/subcontractors will be included in the CITIS, and CITIS data delivery.

5.1.1 -- CITIS Program-Specific Data Repositories

A major decision that must be made early in the planning process is where the data will reside. The data can reside at either a government facility or the contractor site. If it will reside at a Government site, that site should be specified in the SOW. If it will be at the contractor site, the Government should not specify the contractor's repository strategy, but rather specify how they need the repository to function. If any programmatic reasons indicate preference for one strategy over the others, that strategy should be specified in the SOW. The main options for program-specific data repository strategies include:

1. Database repository resides with the prime contractor as a single physical integrated database.
2. Database repository resides with the prime in the form of distributed multiple databases with a navigator.
3. Database repository resides with the prime; existing information systems are interfaced to extract CITIS data in a central repository.
4. Database repository resides with the prime and suppliers (many), with a navigator (gateway processor) to pass requests/access to supplier databases.
5. Database repository resides at a Government facility.

The final repository strategy selected will typically depend on the required CITIS functionality, the existing Government and contractor infrastructure, and the budget available for CITIS development.

5.1.2 -- CITIS and Suppliers/Subcontractors

In keeping with the current shift in attitude toward telling contractors what needs to be done rather than telling them how to do it, the SOW should specify simply that the Gov't. will (or will not) require access to supplier/subcontractor data via the CITIS. The contractor should then decide how they want that data delivered.

The four methods for incorporation of subcontractor data into the CITIS include:

1. Subcontractor delivers data on paper -- prime scans it in and adds it to CITIS in raster format.

2. Subcontractor delivers data via physical media in digital format -- prime loads it into CITIS.

3. Subcontractor downloads its data directly into CITIS databases.

4. Subcontractor becomes member of CITIS network and users have access to all of its data.

5.1.3 -- CITIS Data Delivery and Acceptance

For most defense programs, a large volume of technical data will be created by the contractor in support of the program. Before this data can be released for access through the CITIS, it must meet the programmatic requirements and pass the contractual restrictions.

Figure 6-3 shows greater detail on the CITIS operational environment. Both the Government and the contractor must take precautions to ensure that data is not released for CITIS access without the appropriate approval. Contractors will typically have a database of working data that is not made available to the Government. This data must pass through a "contractual and programmatic filter" to determine whether the data content satisfies the program requirements and the data format meets the contractual restrictions before it is released to the Government. This process is no different from the current paper-based method of data delivery; it is simply performed electronically rather than on paper. When preparing its CITIS approach, the contractor will also need to consider how data that has been delivered to the Government but has not yet been accepted should be handled to prevent data users (other than those reviewing the deliverable) from accessing and using that data prematurely.

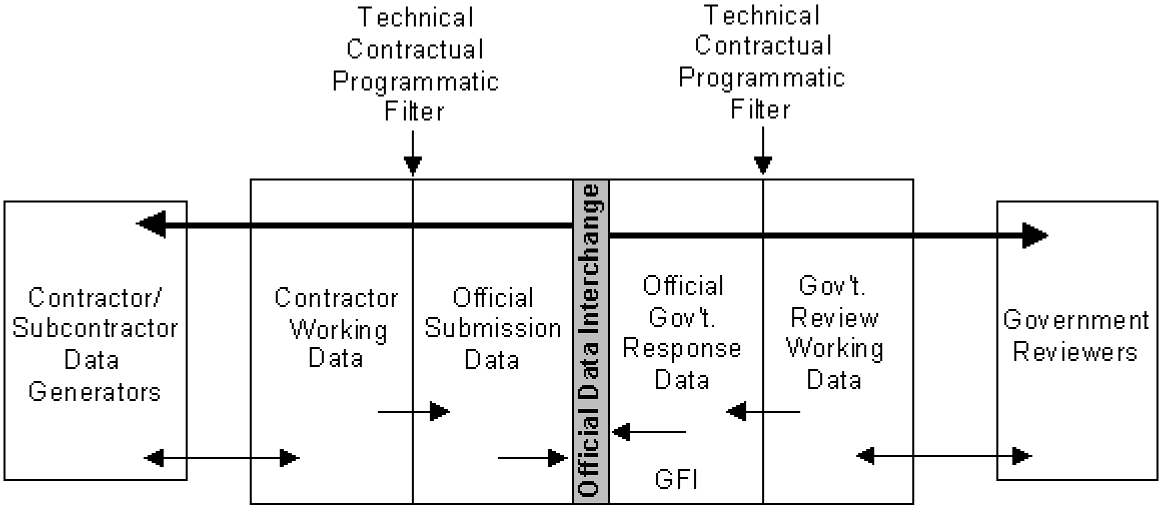

Figure 6-3. -- CITIS Operational Environment.

The contract must address the questions of what constitutes data delivery, and who in the Government will receive, inspect, and accept the data. The Government will specify in the contract the delivery methods for each CDRL item, and if delivery includes CITIS, this delivery may be in the form of either in-place delivery, in which the data item is considered delivered once it becomes available on the CITIS, or it may be in the form of a physical data download by the Government from the CITIS.

The following scenario identifies the steps taken by a typical program office in the receipt, review, and acceptance of digital data delivered in a basic CITIS environment. This scenario assumes that the program uses a local Government server as the respository for data under review, and uses the contractor site as the repository for officially approved and released versions of data deliverables:

1. Data Manager receives notice (via E-Mail) from the contractor that the data item is ready for transfer/download from the contractor's server, along with information about the data item (e.g., file location and name).

2. Data Manager transfers/copies the data file from the contractor's designated location to the designated Gov't. server location via a direct network connection or through telecommunications.

3. Automated Data Processing (ADP) person inspects file for viruses, corruption, etc., verifies the data content and format, and renames the file according to a pre-determined naming convention. Note that this person only verifies that the file contains the information it is supposed to, not the technical content itself.

4. ADP person places file in designated location on server, and implements any access restrictions.

5. ADP person notifies Data Manager that file has been successfully downloaded and provides file name, location, and size.

6. Data Manager notifies contractor via E-mail that file has been received (officially delivered).

7. Data Manager notifies users that the file is now available on the network, file location, file name, file size, and point of contact for that data item.

8. Data item reviewers locate, view, and/or transfer data files as appropriate.

9. Remote users use FTP or TELNET to download files to their location.

10. Reviewers generate comments in a selected format.

11. Reviewers send comments to data item point of contact for collation and delivery to contractor.

12. Data item point of contact reviews and collates comments and passes them on to the Data Manager via E-mail or network.

13. Data Manager transfers comments to designated contractor network location and notifies contractor via E-mail that comments have been delivered.

14. Contractor incorporates comments as necessary and resubmits document.

After the final document is approved for release, the contractor would place the document in an agreed upon location on its server and make it available to all authorized users.

5.2 -- Infrastructure Considerations

The selection of hardware and software used to create the CITIS is critical and must be thoroughly analyzed before any attempt to develop CITIS is begun. The CITIS configuration should be determined only after analysis and comparison of the Government's and contractor's infrastructures. Some important considerations include compatibility of operating systems, file formats, and hardware and telecommunications options. The CITIS designer should also consider future impacts to the CITIS system should Government users upgrade their hardware or software.

When determining the infrastructure for CITIS, the program manager must decide whether the contractor or the Government or both will provide the hardware and telecommunications for the Government to interface with CITIS. Typically, the Government will use its own computer hardware and software to access the CITIS data, with the contractor providing only the software necessary to access CITIS. However, the program manager may choose to have the contractor provide computer hardware (e.g., complete PCs, terminals, etc.) and/or software to be located at Government facilities and used exclusively for CITIS access. This option may be especially attractive for locations that could otherwise require infrastructure upgrades to access CITIS.

An inexpensive CITIS alternative involves data item delivery in place to a Government server located at a contractor site. This server could be maintained remotely by a Government system/database administrator. This is an inexpensive method to implement CITIS. In this scenario, the SOW would have to identify the Government Furnished Equipment (GFE) and specify delivery in place of the data items. An actual Army program that successfully implemented this type of CITIS is described below.

The PM Combat Mobility Systems (CMS) implemented this type of CITIS for their IDE project. In this case, a Government-furnished Unix file server was placed at the contractor's facility and an existing T1 line, which was leveraged from another program, connected the PM with the contractor site. The Government provides system, database and technical support for the remote servers in the IDE, as well as those at the PM's location. The file server at the contractor site is outside their firewall and is accessible through their LAN. Therefore, delivery and exchange of data is accomplished by placing information on the server. Accessing the data is accomplished, in this case, by the JCALS Workflow Manager or Reference Library. This scenario eliminates all overhead on the weapon system contract associated with providing and maintaining a CITIS and thereby lowers the production cost of the weapon system.

<u>5.2.1 -- Hardware and Software</u>

Implementation of an IDE, including CITIS, can range from the very simple to the highly complex. Every CITIS should make maximum use of existing infrastructure in order to minimize costs and reduce the potential user resistance to new processes and technology.

The basic hardware and software used by most CITISs includes:

- PC Workstations
- Servers
- Network connections (LANs and WANs)
- E-mail software
- Modems and phone lines (if no direct network connection to contractor) plus communications software
- CITIS data access software to provide data query, indexing, and navigation capability

Additional infrastructure that could increase functionality include:

- Dedicated high speed lines (ISDN or T1)
- COTS applications for processing data on-line
- Data conversion software
- Optical drives for archiving data onto CD-ROM
- Software to provide functions such as on-line comment and approval, digital signature, etc.
- Enhanced data security, including encryption hardware and software, firewalls, public and private keys, etc.
- Workflow management software
- Configuration management software

A fairly new method for providing basic CITIS capabilities is a contractor-developed and maintained intranet. The concept of the intranet is becoming increasingly popular as a means to provide restricted Internet access to data and information. Intranet-specific technology includes internet technology but adds filtering and security. An intranet usually carries the additional restriction that users allowed access to critical data sources be part of a limited collection of hosts. An intranet would allow users to locate, view, download, and print data items via the familiar mechanism of home pages. Use of an intranet would require the basic CITIS infrastructure listed above with the addition of web browser software for users (e.g., Netscape), and web development software for contractors (e.g., HTML authoring).

5.2.2 -- Networks and Telecommunications

The simplest means of transferring data between the contractor and Government is to connect the appropriate locations with a Wide Area Network (WAN). Several WANs have been and will be implemented that incorporate both contractor and Government facilities.

When networks are not available, users must utilize telecommunications, which involves the physical connection to CITIS via telephone or other type of lines. The CITIS access can be via regular phone lines, dedicated modem lines, high-speed optical lines, or networks, and will typically be a combination of these methods. See Section 3 of this Desktop Guide for a general discussion of digital data infrastructure. Many Government facilities either presently have or are installing the infrastructure required for remote access and electronic data transfer, and no additional telecommunications lines or hardware will be required for CITIS access. If, however, any new lines or networks will be required, the program manager must decide whether the Government or the contractor will be responsible for line installation and maintenance. The Government will typically pay for its own connection time charges (e.g., phone line usage) for use of its own telecommunications lines. The Government may, however, require the contractor to establish an 800-number hotline that can be used by the specified number of concurrent CITIS users.

5.2.3 -- File Format Considerations

Before any CITIS development is performed, the Government and contractor must determine the data formats that will be available on-line. A matrix should be developed during the CITIS planning stage showing which software tools will be used and how the Government (GFI) and contractor data will be stored and displayed. An ideal CITIS would be able to display and process data in any format, regardless of the software tool used to develop it. However, this ideal CITIS may be economically prohibitive and technologically challenging. In practice, the Program Manager will need to specify a limited number of formats for data delivery, including any or all of the following options:

- Mutually Agreeable Commercial Software (MACS) formats (e.g., common word processing formats)
- CALS and/or commercial standard formats (e.g., IGES, SGML, etc.)
- Neutral data formats (e.g., Adobe Acrobat's Portable Document Format [PDF])

Each format is recommended for different reasons and for different types of files. A thorough discussion of these recommendations can be found in paragraph 3.6 of Section 5 and paragraph 3.0 of Section 9 of this Desktop Guide. In practice, some programs request data deliveries in multiple formats. For example, a report could be delivered in its native format (word processing) as well as in a neutral data format (PDF). The file in its native format would be maintained for future updates, while the neutral data file would be made available to reviewers and data users, who could do everything they need to with the file except change it.

The Program Manager must also keep in mind that different formats may be specified for new data and legacy data. Legacy data is technical data that was developed and archived before the implementation of CALS initiatives. New data will typically be in one of the three formats listed above. Depending on its anticipated use, legacy data can be retained in its original native format (typically paper or aperture cards), scanned in and stored in raster or neutral data format, or recreated as a processable file.

5.2.4 -- Infrastructure Changes

Because of the rapidly changing computer hardware and software technology, it is reasonable to assume that at some point during the life of the CITIS, the Government users will upgrade either their hardware or software or both. The Government and the contractor should agree up-front as to what technology refreshments the Government can expect the contractor to incorporate after the CITIS has been implemented. The Government may also want to state explicitly that CITIS shall be upgraded to be compatible with any major changes in hardware and/or network configuration. CITIS user group meetings can serve as an excellent forum for discussion of compatibility problems, technology advancements, and the advantages and disadvantages to upgrades to the CITIS.

6.0 -- CITIS Issues

When CITIS is being considered and/or developed, the program manager must be aware of some of the legal issues accompanying the use of a CITIS. The relationship between CITIS and the future JCALS and Defense Shared Data Warehouse (DSDW) initiatives should also be considered when determining the scope and functionality of the CITIS, to reduce the number of possible conflicts when these systems are finally implemented.

6.1 -- Legal Issues

Because CITIS can involve extensive sharing of data between contractors, subcontractors, and Government activities, a significant number of legal issues have been raised and are still being debated. Some of the most prevalent issues include the questions of proprietary data rights (who owns the data when), software licensing, warranties and liabilities, and international data exchange.

6.1.1 -- Proprietary Data Rights

The extent and nature of rights which the Government may acquire to use, copy, or disclose data items shall be as expressly stated in the contract. In general, according to DFARS 252.227-7013:

The Government shall have unlimited rights in technical data that are --

(i) Data pertaining to an item, component, or process which has been or will be developed exclusively with Government funds;

(ii) Studies, analyses, test data, or similar data produced for this contract, when the study, analysis, test, or similar work was specified as an element of performance;

(iii) Created exclusively with Government funds in the performance of a contract that does not require the development, manufacture, construction, or production of items, components, or processes;

(iv) Form, fit, and function data;

(v) Necessary for installation, operation, maintenance, or training purposes (other than detailed manufacturing or process data);

(vi) Corrections or changes to technical data furnished to the Contractor by the Government;

(vii) Otherwise publicly available or have been released or disclosed by the Contractor or subcontractor without restrictions on further use, release or disclosure, other than a release or disclosure resulting from the sale, transfer, or other assignment of interest in the technical data to another party or the sale or transfer of some or all of a business entity or its assets to another party;

(viii) Data in which the Government has obtained unlimited rights under another Government contract or as a result of negotiations; or

(ix) Data furnished to the Government, under this or any other Government contract or subcontract thereunder, with --

(A) Government purpose license rights or limited rights and the restrictive condition(s) has/have expired; or

(B) Government purpose rights and the Contractor's exclusive right to use such data for commercial purposes has expired.

When dealing with intellectual property, there is an increased risk of misuse of proprietary and business sensitive data in digital form. No DoD regulation currently exists to assess liability on third parties for copyright or patent infringement. Even with access limitations, proprietary markings, such as proprietary legends and restrictive distribution statements, may be inadvertently deleted. The problem could be compounded if the CITIS network includes access by other contractors and subcontractors in addition to the prime contractor, because the release of proprietary data to widely accessed databases could amount to abandonment of secrecy with a resultant loss of rights. Finally, there is the potential problem where Contractor A doesn't want Contractor B to have access to its data, but it can be difficult to prevent that access on a robust CITIS network. All of these issues should be considered and discussed by the Government and the prime contractor in the early stages of CITIS planning.

6.1.2 -- Software Rights/Licensing

Potential third party licensing problems can arise whenever CITIS is used to launch/access other applications. If the applications being accessed are commercial software packages, the contractor will need to investigate the licensing policies of the software development company. In some cases, they may need to either purchase individual licenses for the maximum number of concurrent CITIS users or purchase a network or site license that allows specified or unlimited usage of the software. If the applications being accessed were developed by either the prime or other DoD contractor, the CITIS developers will need to verify that the application has been released for general use. If access is restricted, those restrictions must be incorporated into the CITIS access rule set that will deny access to anyone without the proper authorization.

Care should be taken to identify and grant access to both commercial and contractor-developed applications only to people who actually require that access in order to avoid excessive license purchases and proprietary data conflicts (i.e., don't just automatically grant all CITIS users access to all applications).

6.1.3 -- Warranties and Liabilities

The contractor warrants that the data provided by them via the CITIS is accurate and complete, but the question of who is responsible for warranting data products created by CITIS users with ad-hoc queries has not yet been answered. The contractor can (and should) be held liable for providing defective data to the Government, but unfortunately, lack of statutory laws results in the contractor also being held liable for misuse of any data they provide. Until existing laws are changed, the contractor is liable for damages when data provided through CITIS is used incorrectly.

6.1.4 -- International Data Exchange

International data exchange is complicated by differences in treatment of intellectual data from nation to nation. Some nations do not recognize or protect intellectual property. Export licensing of technical data also creates a barrier to international CITIS implementation. Any data to be released internationally needs prior Government approval.

Section 7
Sample Statement of Work (SOW)
Language and Source Selection Criteria

1.0 -- Introduction

This Generic Statement of Work (SOW)/Statement of Objectives (SOO) provides sample language to assist in the implementation of Continuous Acquisition and Life-cycle Support (CALS) and for the development of a CITIS for an acquisition program. The content within each sample paragraph should be tailored for each application. This CALS-related language should be used in developing the functional requirements within each applicable section of the Request For Proposal (RFP) or Request for Quotation (RFQ) SOW. This language is not intended to be inserted as a stand-alone section within the RFP/RFQ SOW. **Note:** throughout this section, the term "SOW" will be used to indicate either a SOW or SOO.

<Bracketed, italic text> indicates program-specific information that must be inserted into the SOW. Text enclose in square brackets [ ] are notes to the reader that are not intended to be included in the SOW.

Note: ***A word of caution about the paragraph numbers illustrated in the sample texts that follow. Paragraph numbering is relative, not absolute. For example, if the solicitation's section C contains more than the digital technical information system requirements illustrated, the paragraph numbers must expand to reflect this fact. Similarly, if the work requirements are moved out of solicitation section C and into a SOW attachment, the other numbering convention of MIL-HDBK-245 would apply. Namely: paragraph 1 is scope, paragraph 2 is applicable documents, and requirements paragraphs are assigned numbers starting with "3".***

2.0 -- Sample Statement of Work (SOW) Language

2.1 -- SOW Para. 1.0 -- Scope

The contractor shall establish a digital technical information (TI) infrastructure to provide automation and integration of the generation, delivery, and uses of <*program name*> technical information over the <*"defense system" or "equipment"*> life cycle. Unless otherwise specified within the contract, all, or any portion of, the technical information (TI) specified herein shall be developed in a digital form compatible with requirements stated herein. Unless specifically stated herein, the following requirements do not replace or amend requirements for delivery of TI in non-digital forms specified elsewhere in the contract.

2.2 -- SOW Para. 2.0 -- Specific Requirements

The contractor shall implement a CALS program that will achieve the following objectives:

a. Implement a contractor technical information system for on-line access to and delivery of programmatic and technical digital data;

b. Authorize Government access to the contractor database(s); and;

c. Deliver technical information in military and industry standard digital forms.

2.2.1 -- SOW Para. 2.1 -- CALS Approach

[see 2.2.2 below for description of the CALS planning document.]

The contractor shall define a specific CALS implementation objective and strategy, taking into consideration technical constraints, quality and cost guidelines and the Government Concept of Operations (GCO) established by the service Program Manager. This strategy shall be supported by necessary trade studies, and shall describe the framework for CALS implementation activities to be accomplished during each phase of <*program name*> system development. The strategy shall define how the program will implement and operate in an Integrated Data Environment (IDE), identify the critical infrastructure and process modifications that will enable the IDE, and provide details on how program risk and costs will be reduced and product quality improved through CALS initiatives. The implementation strategy shall serve as a guide in developing contractual requirements for later program acquisition phases. This CALS approach shall be detailed in the <*name of CALS planning document*>.

2.2.2 -- SOW Para. 2.2 -- <*name of CALS planning document*>

[This document is optional, and is typically the CALS Implementation Plan (CALSIP). Regardless of what it is called, a CALS/IDE planning document is recommended to ensure successful CALS implementation.]

The contractor shall develop and maintain a current, comprehensive and detailed <*name of CALS planning document*> outlining the procedures to be used to accomplish the CALS requirements defined in <*Section X.X*> of this Statement Of Work (SOW). The <*name of CALS planning document*> shall address capabilities for automating the access and retrieval of technical data, and provide for digital exchange and integration between the engineering, manufacturing, logistics and other functional areas as appropriate to this acquisition phase of the program.

The <*name of CALS planning document*> shall address, as a minimum, the following:

- CALS support hardware and software architecture, reference documents, points of contact.
- Contractor's approach and experience in creation, management, use, and exchange of digital information.
- Contractor's capabilities for integrating applications and databases.
- Procedures to improve product quality and eliminate data redundancy.
- Proposed CITIS on-line access capabilities.
- Information system and relationships with Government receiving systems.
- Outline of proposed actions and capabilities to be pursued in subsequent life cycle phases.

- Telecommunications data protection and integrity, including system security.

The <*name of CALS planning document*> shall be updated every <*number of days/months*> throughout the life of the contract. The updates shall define implementation plans for the upcoming period in greater detail, resolve outstanding strategy issues, respond to strategic and technology changes, and recommend specific alternative approaches for continuation of CALS in the next phase.

2.2.3 -- SOW Para. 2.3 -- Database Architecture/System Tradeoffs

The contractor plan shall provide a cost effective method of managing the utilization of the contractor set of automated data processing systems and applications which support specific weapon system technical database(s) such that appropriate configuration and version control of technical information is maintained, while providing current data for design, engineering analysis, manufacturing, and product support planning. The contractor shall conduct appropriate tradeoffs/studies/analyses to support determination of the CALS implementation strategy. The status of these studies shall be reviewed at appropriate program reviews, and the results documented as part of the <*name of CALS planning document*>. Candidates for such studies include:

(Examples only; final determination is program specific)

- improved alternate data generation and delivery modes
- infrastructure compatibility and recommended upgrades
- digital data delivery vs. on-line access
- analysis of telecommunication alternatives
- functional integration cost/benefit studies

2.2.4 -- SOW Para. 2.4 -- Security

[If a CALSIP or other CALS planning document is not being required, the contractor needs to address this security information in some other specified deliverable.]

The contractor shall establish a security system and enforce data protection and integrity standards. System security engineering principles as outlined in <*specify security document, typically MIL-STD-1785*> shall be used. Controls to prevent unauthorized access shall be established and detailed in the <*name of CALS planning document*>. The plan shall be based on the results of documented data protection and integrity, threat and vulnerability analysis, risk assessments, and tradeoff analyses. Vulnerabilities that remain after security system design shall be identified. The plan shall include disaster recovery provisions. Security requirements that must be complied with by Government personnel will be identified to the Government in the security section of the <*name of CALS planning document*>. Any peculiar software that must be resident on Government access terminals will be provided and maintained by the contractor.

Information requiring special security provisions such as classified data, critical technology and sensitive data, such as proprietary, competition or liability sensitive data, will be partitioned to minimize the volume of information requiring specialized handling, to provide classification at the lowest classification level, and to control access. Sensitive data, in this context, includes but is not limited to, CDRL data items marked with one or more of the following: an export control warning notice, restrictive distribution statement (i.e., distribution statements B, C, D, E, F or X) and/or a proprietary legend from the FAR or DFARS. Encryption of classified data or sensitive military data shall be stipulated by the CDRL and on an as-required basis in accordance with procedures established by the National Security Agency. Such information shall be identified to prevent inadvertent disclosure and retention of security identification for printouts of accessed information. The contractor shall pay particular attention to unclassified items of information, which, taken together, can infer classified information.

The contractor shall maintain configuration control of the security system and trusted system components. The contractor shall conduct a test and evaluation of the system and periodic inspections to ensure compliance. The Government shall retain the right to conduct announced and unannounced inspections by security specialists at any time to review, audit, and account for classified materials.

2.2.5 -- SOW Para. 2.5 -- Program Assessment and Control -- Department of Defense (DoD) Reviews

The <*name of CALS planning document*> shall describe the procedures and controls by which the contractor and the Government will evaluate the status and effectiveness of CALS. The implementation of CALS will be a subject of review at various program reviews.

2.2.6 -- SOW Para. 2.6 -- Post Award Planning Meetings

The prime contractor shall host a post award CALS program orientation conference to be scheduled no later than <*number*> days after contract award. A representative from the <*program name*> program office shall chair this conference. Major prime contractor teaming partners/subcontractors shall attend. The agenda for this conference shall be approved by the <*program name*> program office. The purpose of this CALS meeting is to clarify the GCO and have the contractor present to the Government their plans for on-line access, if required, exchange, and delivery of digital data.

Additional CALS meetings shall be conducted at <*number of months*> intervals to discuss the status of CALS implementation efforts. These meetings will provide a forum for Government and contractor discussion and resolution of problems with infrastructure, data formats, data interchange, and systems integration.

2.2.7 -- SOW Para. 2.7 -- Government Furnished Information (GFI)

The list of GFI the Government plans to provide is included in attachment/exhibit <*number*>. GFI shall be provided in digital format except in cases where hard copy is the only available media. The GCO will define infrastructure capabilities to receive and use various types of digital data and technical information. GFI provided in digital format shall be available for on-line access, except in cases where file sizes or formats are prohibitive.

2.3 -- SOW Para. 3.0 -- Contractor Integrated Technical Information Services (CITIS)

[General Description: see paragraph 3 for a standalone detailed CITIS SOW.]

The contractor shall propose ["develop" if Section C SOW requirement] a program composed of procedures, processes, specifications, computer and telecommunications equipment, and software applications for the integration, storage, exchange, and/or on-line sharing of data with the Government. These technical data and database(s) and functional application capabilities provided within the contractor's system shall be referred to as the CITIS. MIL-STD-974, Attachment <*number/letter*>, may be used as guidance for CITIS development. This CITIS shall be developed in accordance with the following.

The contractor shall propose ["develop" for Section C SOW requirement] a Technical Information (TI) and program management architecture, with a functional and hierarchical indexing system to:

- Manage configuration of the entire TI and planning databases,
- Integrate planning information into its respective TI source database; and
- Trace configuration changes from design to logistics products and vice versa.

The contractor shall propose how he will ["is required to" for Section C SOW language] establish a link among logistics, design, engineering, and manufacturing data and functional processes to facilitate the interchange and exchange of technical information; integrate technical data and database(s) to support the design, manufacturing and support processes and allow for timely access by authorized Government activities; provide an integrated, shared data environment, consisting of integrated databases, analysis tools, and engineering processes designed to utilize digital TI; and, provide for the generation, storage, indexing, distribution, and delivery of integrated acquisition and logistics information products. The contractor shall leverage existing CITIS capabilities and resources, and maximize commonality and reuse of CITIS software and hardware to achieve an optimum solution. In the selection of analytical tools, the contractor shall maximize the use of previously developed or off-the-shelf software. These software tools shall be compatible with Government hardware/software systems stated in the GCO, unless contractor developed, unique software solutions are demonstrated to be more cost effective.

2.3.1 -- SOW Para. 3.1 -- Data Element Dictionary

[If CITIS is required.]

A general data element dictionary shall be developed so that identical data elements are addressable by the computer as the same data element. Changes to any duplicate data element shall be effected throughout all databases. A similar methodology shall be developed for graphics and large textual entities to ensure that changes to the source graphic correctly flags the necessity for change to all dependent graphic/textual entities derived from the source graphic.

2.4 -- SOW Para. 4.0 -- Engineering Data (Graphic and Text Files)

Any data, either Government, contractor, or vendor, that contains engineering definition or guidance on material items (components), equipment system practices, methods, and/or processes relating to the design, manufacture, acquisition, test, inspection shall be submitted in digital form in accordance with the CDRL and compatible with the Government data repository/receiving systems stated in the GCO.

[The following paragraphs contain language that should be integrated with the specific functional area that it addresses.]

2.5 -- SOW Para. 5.0 -- Automation & Functional Integration

The contractor should use computer-aided design, engineering, and manufacturing methods (CAD/CAE/CAM) to support design integration with manufacturing planning and logistic support system development. These software tools shall be compatible with the Government hardware/software systems stated in the GCO, unless contractor developed, unique software solutions are demonstrated to be more cost effective. An integrated set of ADP systems and applications will be used by the contractor team to enter, update, manage, and retrieve data from specific <*program*> technical database(s).

2.6. -- SOW Para. 6.0 -- Diagnostics

The source of diagnostic information will reside in logistics engineering databases offering data exchange in neutral formats. Software shall be developed to provide for automated interface with in-service performance and maintenance data collection processes and to provide feedback concerning successes and failures in the fault isolation process to the system designer. Diagnostic systems that learn from experience and which have the capability to update a knowledge-based diagnostic database to optimize the fault isolation process or to improve system design are to be used to the fullest extent possible.

2.7 -- SOW Para. 7.0 -- Management Information Tools

The contractor shall establish an on-line direct access capability for recording, planning, scheduling, and reporting status of program requirements. This shall provide visibility of the contractor's performance, highlight potential problems, and provide schedule compatibility checks to ensure integration of functional activities. This on-line capability shall identify change impacts on related areas of logistic support, design and manufacturing, and provide the status of program deliverables.

2.8 -- SOW Para. 8.0 -- Technical Manuals/Technical Orders

The contractor shall provide for computer assisted generation of technical manuals/technical orders. This data is to be derived, to the maximum extent possible, from integrated digital data files, e.g., CAD/Engineering database. The development of Interactive Electronic Technical Manuals (IETMs) shall be explored and instituted when determined to be cost-effective and advantageous to the presentation of the material. This data shall be provided in accordance with <*Service-unique specifications and TM/TO development guidance or other TM/TO SOW requirements*>.

2.9 -- SOW Para. 9.0 -- Supply Support

The contractor shall maintain spare parts identification consistent with the approved configuration baseline and allow for on-line assessment of the impact to spare parts requirements during analysis of design alternatives. The contractor shall provide provisioning technical documentation to facilitate automated ordering, supply management, and distribution, and should provide on-line identification of spares, repair parts, and source/maintenance/recoverability coding. This data shall be provided IAW <*Service-unique specifications and TM/TO development guidance or other TM/TO SOW requirement*>.

2.10 -- SOW Para. 10.0 -- Training

Training design, production, and delivery will be guided by the processes of the Systems Approach to Training (SAT) or the Instructional Systems Design (ISD). A thorough analysis of the training needs of the target audience, the tasks to be trained, and the most cost effective media must be conducted early in order to facilitate an integrated development process. Maximum use of preliminary training documents and training sessions will ensure the finalized training support package meets the needs of the user audience. Electronic training technologies such as video-teleconferencing and computer-based training shall be used to the maximum extent possible to enhance the effectiveness of training materials and courses.

Next Section